UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,730	03/31/2004	Bruce Edward LaVigne	200314975-1	5129

22879 7590 05/03/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	**PAPER NUMBER**
2132	
MAIL DATE	**DELIVERY MODE**
05/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,730	LAVIGNE ET AL.	
	Examiner	Art Unit	
	Devin Almeida	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/31/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 3/31/2004. Claims 1-23 were received for consideration. No preliminary amendments for the claims were filed. Currently claims 1-23 are under consideration.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 3/31/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1,2, 7-9, and 14-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Amara et al (U.S. Patent # 6,839,338). Amara teaches with respect to claim 1, a method for secure remote mirroring of network traffic, the method comprising: receiving a data packet (see column 8 line 66 – column 9 line 15 i.e. IP packet) to be remotely mirrored by an entry device (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet) pre-configured with a destination address to which to mirror the data packet; encrypting the data packet to form an encrypted packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet); generating and adding a header to encapsulate the encrypted data packet, wherein the header includes the destination address (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet); and forwarding the encapsulated encrypted packet to an exit device associated with the destination address (see column 8 line 66 – column 9 line 15 i.e. the new IP packet is then sent through the network to a destination device endpoint).

With respect to claim 2, wherein the destination address comprises an Internet protocol (IP) destination address (see column 9 lines 16-40), wherein the header comprises an IP header (see column 8 line 66 – column 9 line 15 i.e. IP packet); and wherein the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet).

With respect to claim 7, further comprising: receiving the encapsulated encrypted packet by the exit device (see column 8 line 66 – column 9 line 15 i.e. the destination device endpoint); removing the header to de-encapsulate the encrypted packet; and decrypting the encrypted packet to re-generate the data packet (see column 8 line 66 – column 9 line 15 i.e. the destination device endpoint decrypts the original IP packet and forwards that packet to the destination device).

With respect to claim 8, wherein the encrypting and decrypting is performed under a public-private key encryption scheme (see column 10 lines 6-60).

With respect to claim 9, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device (see column 10 lines 6-60).

With respect to claim 10, configuring the entry device in a best effort mirroring mode to reduce head-of-line blocking (see abstract and column 8 line 66 – column 9 line 15).

With respect to claim 11, configuring the entry device in a lossless mirroring mode to assure completeness of mirrored traffic (see abstract and column 8 line 66 – column 9 line 15).

With respect to claim 14, a networking device comprising: a plurality of ports for receiving and transmitting packets therefrom (see column 8 line 66 – column 9 line 15 i.e. IP packet); a secure remote mirroring engine (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint) configured to detect packets from a specified mirror source, to encrypt the detected packets (see column 8 line 66 – column 9 line 15 i.e. the

source device endpoint encrypts the IP packet), to encapsulate the encrypted packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet), and to forward the encapsulated encrypted packets to a pre-configured destination by way of at least one of the ports (see column 8 line 66 – column 9 line 15 i.e. the new IP packet is then sent through the network to a destination device endpoint); and an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet).

With respect to claim 15, wherein the destination comprises an Internet protocol (IP) destination address (see column 9 lines 16-40).

With respect to claim 16. The networking device of claim 15, wherein the remote mirroring engine encrypts the packets using a public key of a public-private key pair (see column 10 lines 6-60).

With respect to claim 17, a system for secure remote mirroring of network traffic, the system comprising: a mirror entry device including a secure mirroring engine configured to detect packets from a specified mirror source (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint), to encrypt the detected packets using an encryption module (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet), encapsulate the encrypted packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet), and to forward the encapsulated

encrypted packets to a pre-configured destination by way of at least one of the ports (see column 8 line 66 – column 9 line 15 i.e. the new IP packet is then sent through the network to a destination device endpoint); and a mirror exit device (see column 8 line 66 – column 9 line 15 i.e. destination device endpoint) including a secure mirroring receiver configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to decrypt the encrypted packets (see column 8 line 66 – column 9 line 15 i.e. the destination device endpoint decrypts the original IP packet and forwards that packet to the destination device).

With respect to claim 18, wherein the encrypting and decrypting is performed under a public-private key encryption scheme (see column 10 lines 6-60).

With respect to claim 19, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device (see column 10 lines 6-60).

With respect to claim 20, a system for secure remote mirroring of network traffic, the system comprising a mirror entry device (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint) including means to encrypt the detected packets using an encryption module (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet) and to encapsulate the encrypted packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet); and a mirror exit device (see column 8 line 66 – column 9 line 15 i.e. destination device endpoint) including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to

decrypt the encrypted packets (see column 8 line 66 – column 9 line 15 i.e. the destination device endpoint decrypts the original IP packet and forwards that packet to the destination device).

With respect to claim 21, A method for secure remote mirroring of network traffic, the method comprising: r remotely configuring an entry device (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint) with an encryption key (see column 10 lines 6-60) and destination address (see column 9 lines 16-40); remotely configuring an exit device (see column 8 line 66 – column 9 line 15 i.e. destination device endpoint) at the destination address with a decryption key (see column 10 lines 6-60); receiving a data packet to be mirrored by the entry device (see column 8 line 66 – column 9 line 15 i.e. the destination device endpoint decrypts the original IP packet and forwards that packet to the destination device); encrypting the data packet using the encryption key to form an encrypted packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet); generating and adding a header to encapsulate the encrypted data packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet), wherein the header includes the destination address (see column 9 lines 16-40); and forwarding the encapsulated encrypted packet to the exit device (see column 8 line 66 – column 9 line 15 i.e. the new IP packet is then sent through the network to a destination device endpoint).

With respect to claim 22, wherein the remote configuration is performed by way of SNMP (see column 3 line 14 – column 4 line 17 SNMP is included in TCP/IP).

With respect to claim 23, wherein the remote configuration is performed by way of a secure remote protocol (see column 3 line 14 – column 4 line 17).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liu (U.S. 2004/0184408) in view of Amara et al (U.S. Patent # 6,839,338). Liu teaches with respect to claim 1, a method for secure remote mirroring of network traffic, the method comprising: receiving a data packet (see paragraph 0020-0021) to be remotely mirrored by an entry device (see figure 1 element 102 Access Node and paragraph 0020-0021) pre-configured with a destination address (see paragraph 0023 i.e. MAC destination address) to which to mirror the data packet; generating and adding a header to encapsulate the encrypted data packet (see paragraph 0023 i.e. MAC –in-MAC packet), wherein the header includes the destination address (see paragraph 0023 i.e. MAC destination address); and forwarding the encapsulated packet to an exit device (see figure 1 element 110 Access Node and paragraph 0020-0021) associated with the destination address (see paragraph 0021 i.e. forwards the data packet and MAC header to destination access switch 110). Liu does not teach encrypting the data packet to form an encrypted packet. Amara teaches encrypting the data packet to form an encrypted

packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have encrypted the data packet to protect to packet while it is sent across the network to the endpoint where it can be (see Amara column 9 line 64 – column 10 line 59). Therefore one would have been motivated to have encrypted the data packet.

With respect to claim 3, wherein the destination address comprises a media access control (MAC) destination address (see Liu paragraph 0023 i.e. MAC destination address), and wherein the header comprises a MAC header (see Liu paragraph 0020-0022 i.e. MAC header), and wherein the encapsulated encrypted packet comprises a MAC-encapsulated encrypted packet (see Liu paragraph 0023 i.e. MAC–in-MAC packet).

Claim 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Amara et al (U.S. Patent # 6,839,338) in view of Kojima et al (5,280,476). Amara teaches everything with respect to claim 2 above but does not teach with respect to claim 4 determining a media access control (MAC) address associated with the destination IP address; generating and adding a MAC header to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC address in a destination field; and transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain. Kojima teaches determining a media access control (MAC) address associated with the destination IP address (see Kojima

column 5 lines 17-35); generating and adding a MAC header to the IP-encapsulated packet to form a MAC data frame (see Kojima column 5 lines 5-16), wherein the MAC header includes the MAC address in a destination field ; and transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain (see Kojima column 5 lines 5-16 i.e. delivers the resulting data to the local area network). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have added a MAC header to the data get to help the data get delivered to its destination across the LAN (see Kojima column 5 lines 17-35). Therefore one would have been motivated to have add a MAC header.

With respect to claim 5, wherein determining the MAC address comprises: determining if a mapping of the destination IP address to the MAC address is stored in an address resolution protocol (ARP) cache (see Kojima column 5 lines 17-35); if so, then retrieving the MAC address from the ARP cache (see Kojima column 5 lines 19-20); and if not, then broadcasting an ARP request with the destination IP address and receiving an ARP reply with the MAC address (see Kojima column 5 lines 17-35). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have added a MAC address to the data get to help the data get delivered to its destination across the LAN (see Kojima column 5 lines 17-35). Therefore one would have been motivated to have add a MAC address.

With respect to claim 6, wherein the IP-encapsulated packet is communicated across multiple intermediate layer 2 domains (see Amara figure 1).

Claim 12, rejected under 35 U.S.C. 103(a) as being unpatentable over Amara et al (U.S. Patent # 6,839,338) in view of Classon et al (U.S. Patent 6,700,867). Amara teaches everything with respect to claim 1 above but does not teach truncating the data packet to reduce a size of the data packet prior to encryption. Classon teaches truncating the data packet to reduce a size of the data packet prior to encryption (see column 20 lines 20-53). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have truncated the data packet to satify memory (buffer) requirements (see column 20 lines 20-53). Therefore one would have been motivated to have truncated the data packet.

Claim 13, rejected under 35 U.S.C. 103(a) as being unpatentable over Amara et al (U.S. Patent # 6,839,338) in view of Engwer (U.S. Patent 6,947,483). Amara teaches everything with respect to claim 1 above but does not teach compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption. Engwer teaches compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption (see column 1 line 52 – column 2 line 6). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have compressed the data packet. Data transmission between the various access points (APs) and their associated mobile units may involve large amounts of data which may take substantial amount of time and processing power to transmit over the air median. Such data transmissions are costly if

the transmitted data is uncompressed.s (see column 1 line 52 – column 2 line 6). Therefore one would have been motivated to have compressed the data packet.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100